A Reliable Covert Channel over IEEE 802.15.4 using Steganography

Ajay Kumar Nain, P. Rajalakshmi
Department of Electrical Engineering
Indian Institute of Technology - Hyderabad, India
Email: ee14resch11001, raji@iith.ac.in

***Abstract*—The proliferation of Internet of Things has propelled the popularization of IEEE 802.15.4 standard. For the secure transmission of confidential data over 802.15.4, multiple encryption-based security techniques have been proposed in the literature. But these techniques do not ensure undetectable communication which is crucial in multiple scenarios like covert military operations. It is not sufficient enough to maintain the secrecy of the data using these techniques as it can arouse suspicion and even the encryption might be defeated by the adversary using advanced methods. For covert data communication, some steganographic techniques have been studied for 802.15.4 but unreliability makes it difficult to use for practical applications. In this paper, we propose a reliable method for covert data communication using redundancy in the direct spread spectrum sequences. We propose a secret acknowledgment and error detection method to ensure reliable communication in the covert channel. Results show that we can transfer confidential data reliably at a significant rate without considerably affecting the performance of primary data reception.**

***Index Terms*—DSSS, IoT, steganography, secret communication, 802.15.4 transceiver**

I. Introduction

Internet of things (IoT) is emerging as a promising technology for various applications. Multiple applications are being developed utilizing this technological advancement [1]. Due to characteristics of IoT devices such as heterogeneity and constrained nature, security is a challenging issue with IoT [2]. With the advancement in computing technologies, the secure and secretly transfer of data over wireless channel is becoming challenging day by day [3]. For secure transmission of the data several encryption schemes have been proposed [4]. These schemes provide basic security services and strength against various attacks like information disclosure, modification, duplication etc. However, encryption based approaches cannot resist the adversary in getting knowledge of the transmission by deducing information from patterns in communication [14]. It is not sufficient enough to maintain the secrecy of the data using these techniques as it can arouse suspicion of the transmission between the legitimate parties. Moreover, if adversary is smart enough to decode the encrypted text than privacy of the data will be exploited. In many scenarios ranging from covert military operation to privacy protection for users, there is a requirement of covert communication which cannot be achieved with encryption based approaches.

To transfer data secretly, steganography is the other approach in which secret message is hidden within a cover carrier in such a way that hidden message is undetectable [5]. Steganography is mostly explored with image, video or audio as a cover carrier. This type of steganography is independent of communication standards as it is performed at application layer [6], [7]. It is useful when the cover message has enough redundancy to hide the secret message. However, the mentioned steganography is not suitable for low power and low data rate applications as it requires comparably a large cover message like image etc. For instance, if a secret message is required to transfer over 802.15.4 than to send a very large cover message like the images is not a feasible solution.

However, to send data secretly some physical layer security approaches have been proposed. These approaches provide information-theoretic security instead of computational security which is provided by upper layer security primitives [8]. These approaches exploit the characteristics of the communication channel and are capable for provide high decoding error at the adversary. However, these approaches have many challenges such as unavailable eavesdroppers Channel State Information (CSI), complex computation, excessive power consumption etc. Moreover, most of these techniques require relay or MIMO systems which require more power consumption and may not be so feasible for 802.15.4 [9],[10],[11].

Considering the above problems, some methods have been proposed in literature for secret communication by utilizing the redundancy of communication standards at different layers such as PHY layer, MAC layer [12], [13], [14]. For instance, the upper layers like MAC layer methods utilize the reserved field in the protocol header for data hiding. On the other hand, PHY layer methods utilize the redundancy of the Direct Spread Spectrum Sequence (DSSS) used for error correction in the communication process. These methods avoid the need for a very large cover message for information hiding. However, these methods have several problems for implementation in practical applications like low capacity of information hiding and unreliability of the secret data transmission. PHY layer performs better than MAC layer in terms of embedding capacity which is the ratio of secret data by primary data. Some steganography methods have proposed the information hiding at the PHY layer using DSSS redundancy. However, the complete scheme with error detection/correction of secret data has not been studied for making a reliable covert channel over 802.15.4. In this work, we addressed the mentioned problem and proposed a new mechanism for covert transmission over

IEEE 802.15.4. The contribution of the paper includes:

1) We analyze error performance of existing methods for secret data communication using DSSS steganography.
2) We propose a reliable method for covert transmission over 802.15.4 with secret frame acknowledgment and error detection mechanism.
3) We analyze the performance of the proposed method in terms of symbol error rate as a performance metrics

The rest of the paper is organized as follows. Section II describes the related work. Section III describes the basic requirements of DSSS steganography and error analysis of the existing method. The Proposed method is described in Section IV. Results and performance analysis are given in section V followed by the conclusion and future scope in section VI.

II. Related Works

Few methods have been proposed to send hidden data over 802.15.4 at various layers. Redundancy of the concerned layer is used for this purpose. At MAC layer, the reserve field in the MAC header has been utilized for embedding the secret data. However, these methods have the drawback of low embedding capacity due to limited reserved space in the header [12], [13]. Another way for secret embedding is utilizing redundancy in the DSSS at the physical layer. The advantage of these methods is high embedding capacity in comparison with other methods.

Some steganography techniques have been proposed for secret data transmission using DSSS redundancy. In [15], authors expanded the PN sequence set for the purpose of anti-jamming. In [16], authors proposed a method such that both transmitter and receiver generate an identical set of PN sequence with a prior negotiation. In [17], coding redundancy of DSSS system is exploited by assigning certain number of bit flipping in a PN sequence to represent the secret data. In [18], authors provide a watermark embedding method for 11-chip PN sequence. They analyzed the throughput of secret data with different number of chip-flipping in the PN sequence. In [19], authors proposed an extended cluster for each 32 bit sequence. However, a reliable system for the covert transmission with secret frame error detection has not been proposed to the best of our knowledge.

III. DSSS Stganography Analyisis

In this section, we discuss the principle and requirements of DSSS steganography followed by analysis of existing method with its error performance in the noisy environment.

A. Requirements for the DSSS Steganography

In IEEE 802.15.4, the standard encodes $k = 4$ bits into $2^k = 16$ symbols and each symbol is mapped to 32 bits long chip sequence. These sixteen PN sequences are quasi-orthogonal and selection of these sequences was performed with the aim of maximizing the hamming distance between any two sequences which reflects the error correcting capability of the DSSS system. In DSSS steganography, this redundancy is used to embed the information in the form of altered chips on the designated positions. If m chips can be flipped in a PN sequence of length 32, the total number of positions is ${}^{32}C_m$. If we exhaustively use all number of positions to represent secret data, we can hide a large number of secret bits per PN sequence. However, this is not feasible in practice as extraction process is time-consuming due to exponentially increment of the number of combinations with m. Moreover, this strategy will not be tolerable to even a single chip error in the complete frame which is very difficult to achieve in realistic wireless channel.

To make the extraction process simple and error tolerable, there should be one extended set of PN sequences associated with original PN sequence. The number of extended PN sequences associated with each standard sequence depends upon the number of secret bits to be hidden per PN sequence. If we want to hide k secret bit per symbol, then extended set of PN sequence will have 16 clusters with 2^k sequences inside each cluster. The extended PN sequences in each cluster should satisfy following properties:

1) The number of one and zeros should be equal in each PN sequence.
2) The hamming distance between any two sequences among all the sequence in the same cluster should be maximum in order to make it tolerable to maximum possible error. For instance, to make it tolerable to 2 chip error per symbol, the minimum hamming distance between any to chip sequence should be more than or equal to 5.
3) The hamming distance between the cluster head and any other sequence in the same cluster should be as small as possible. This is to ensure the minimum degradation of the performance at the unaware receiver.
4) The hamming distance between any sequence from one cluster to any sequence from other clusters should be as large as possible.

The property 2 puts a lower limit on minimum hamming distance while properties 3 and 4 put restrict the increment of hamming distances. So there is a trade-off between the two, and extended set should be generated by maximized minimum hamming distances. Xiang Li et al. proposed a similar method for 11-chip PN sequences [18]. For 32-chip PN sequence, Mehta A. et al. proposed an extended set for k=5 [19]. In the following subsection, we analyze the performance of the steganography using this code set. The discussion of the proposed method is followed in the next section.

B. Analysis of Existing Method

In [19], the extended set have 32 PN sequences associated with each original PN sequence as k is 5 in this case. The set of PN sequences is represented by 32-bit hexadecimal values and denoted by $C_{i,0}$ to $C_{i,31}$ for $i = 0$ to 16. The set for $i = 0$ is listed in Table I. The remaining clusters can be generated by the circularly shifting like in originally 802.15.4 codes. To check the performance of the steganography using these codes, we first analyze the hamming distance of each codes listed in the table from each of the codes in original 802.15.4. From

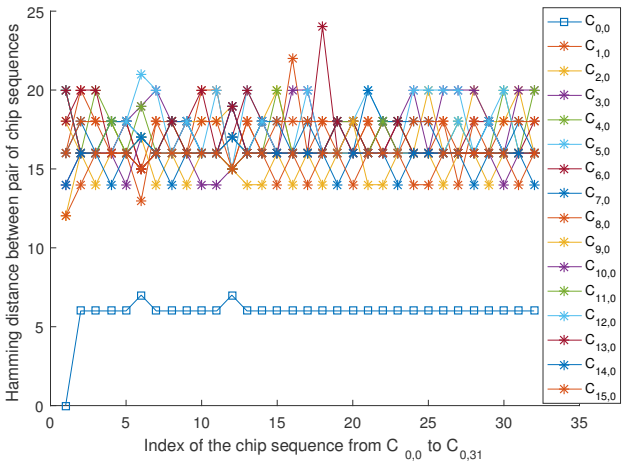

Fig. 1: Hamming distance analysis

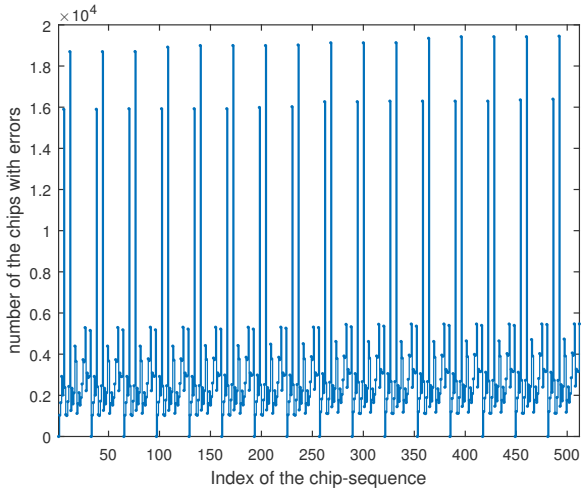

Fig. 2: Number of chips with error in main symbols

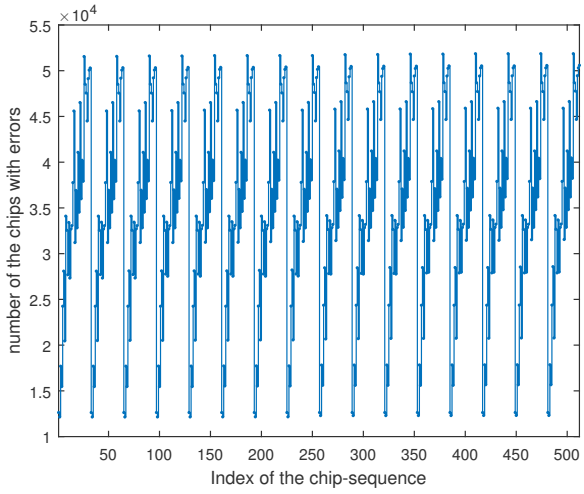

Fig. 3: Number of chips with error in secret symbols

the result which is given in Fig. 1, we observe that hamming distance from the own cluster head is 6 or 7 while the distance from the other cluster head is more than 14. These constraints make it less tolerable to errors introduced in the channel and make it detectable at the unaware receiver.

TABLE I: Extended Code Cluster

$C_{0,0} = d9c3522e$	$C_{0,16} = 5bd350aa$
$C_{0,1} = 19e3da2a$	$C_{0,17} = 5ce3d02e$
$C_{0,2} = 31f3522e$	$C_{0,18} = 91d2da2e$
$C_{0,3} = 45c35a2f$	$C_{0,19} = c1b3d22e$
$C_{0,4} = 4983da6e$	$C_{0,20} = c3c3d06e$
$C_{0,5} = 49d74a2a$	$C_{0,21} = d0d3d42e$
$C_{0,6} = 515b526e$	$C_{0,22} = d1c38b2e$
$C_{0,7} = 51935a3e$	$C_{0,23} = d1d3d2a2$
$C_{0,8} = 51d3512f$	$C_{0,24} = d1eb1a2a$
$C_{0,9} = 51e7c22e$	$C_{0,25} = d1f35246$
$C_{0,10} = 53e3126e$	$C_{0,26} = d5c3926a$
$C_{0,11} = 55c2546e$	$C_{0,27} = d913d82e$
$C_{0,12} = 58f35a26$	$C_{0,28} = d9c7c82a$
$C_{0,13} = 59c3196e$	$C_{0,29} = d9d39a24$
$C_{0,14} = 59d35c2c$	$C_{0,30} = d9f2580e$
$C_{0,15} = 59e34a4e$	$C_{0,31} = ddd3d00c$

To check the error tolerance of the above method, we used all the possible chips with error assuming that original 802.15.4 transceiver is tolerable to 5-bit errors. The total numbers of chip sequences with error locations are $\sum_{k=0}^{5} {}^{32}C_k = 242825$. So, there are 242825 possibility for each transmitted stego-sequence where total number of stego-sequences is of $32 * 16 = 512$ as there are 32 sequences in each cluster. The number of stego-sequences which have been detected wrongly is given in Fig. 2 and 3. In the first figure, total number of sequences which led to wrong detection of main symbols is given. The latter figure represents the number of sequences which led to wrong detection of secret symbols. From Fig. 2, it can be inferred that the performance at the unaware receiver degraded sufficiently by embedding process. Similarly, from Fig. 3, it can be inferred that secret symbols have huge error rate and make this scheme unreliable for secret data transmission due to unavailability of any error detection mechanism for the secret frame which is hidden in the main frame. Even if a single error occurs in secret data in the frame, the complete secret frame will be corrupted.

IV. Proposed Method

In this section, first we discuss working principle of the proposed method. Next subsection describes the transmitter and receiver processes. In the following subsection, we discuss the secret acknowledgment and frame error detection of the covert channel.

A. Working Principle

In the proposed method, we use only a set of 4 sequences in the cluster of each main symbol. This results 2-bit per symbol embedding capacity which can be considered sufficient as the secret data can be transferred at a rate of half of the standard data rate in 802.15.4. This rate of secret data is compromised for better throughput of secret data. The set of the sequence

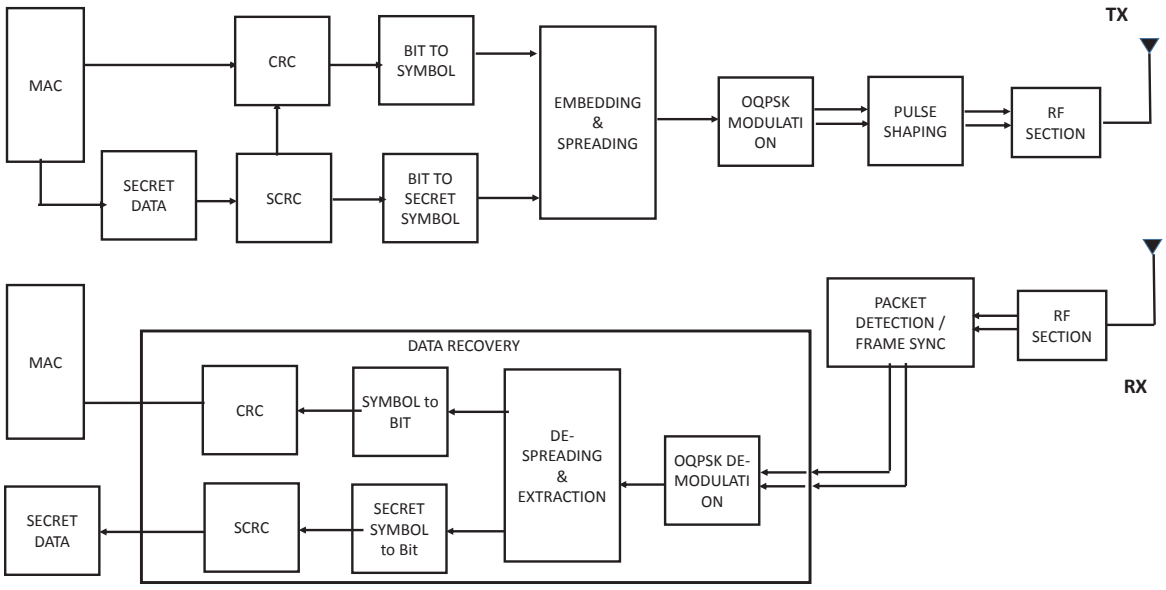

Fig. 4: Block Diagram of Proposed Transceiver

is given in Table II for the $i = 0$. For $i = 1$ to 7, it can be generated by circularly shifting of 4 bits. For $i = 8$, it can be generated by flipping alternate bits similar to the standard 802.15.4. Again for $i = 9$ to 15, it can be generated by circularly shifting of generated sequence for $i = 8$.

TABLE II: Extended Code Cluster for Proposed Method

$C_{0,0} = D9C3522E$	$C_{0,2} = 51935A3E$
$C_{0,1} = 19E3DA2A$	$C_{0,3} = 51D3512F$

For checking the correctness of the secret message, a Cyclic Redundancy Check (CRC) is calculated for secret data and we call it as secret CRC. This secret CRC ($SCRC$) is transferred through the main channel. The reason for sending the $SCRC$ through main channel instead of secret channel is to ensure high confidentiality in correctness of the $SCRC$ value as the secret channel is less tolerable to noise. If the secret message is received correctly, a secret ACK ($SACK$) will be sent to transmitter. If transmitter receives this ACK for the previous frame, it will send the next secret data otherwise it will send the same message again in the next frame. In this way, a reliable secret channel is created along with the main channel of 802.15.4. We call secret symbols and main symbols to the data transmitted over the secret channel and main channel respectively.

B. Transmitter

The flow diagram of the proposed transmitter and receiver is depicted in Fig. 4. At the transmitter, when it gets data from the MAC layer to transmit, the length of the secret data that can be embed into the current frame is decided according to the length of the MAC layer payload. Then it is passed through CRC block which calculates a cyclic redundancy check for error detection purpose. Similarly, for error correction of the secret data $SCRC$ is calculated by SCRC block. The calculation of the $SCRC$ is completed first and the value is attached to the PPDU as last 2 bytes. The spreading and embedding block takes both main symbol and secret symbol as input. This block send 32-bit chip sequence associated with each pair of main and secret symbols. In the embedding process, if secret symbol is zero then there is no effect on the outgoing chips. Otherwise the outgoing chip sequence is one of the chip sequences from the associated cluster of main symbol. The outgoing chips from the mentioned block are modulated and then communicated to RF section through the pulse shaping block.

C. Receiver

At the receiver, first of all, the packet detection and frame synchronization is performed using the PHY header. If a valid frame is detected, the data recovery block is activated in which the incoming symbols are first demodulated. Then the resulting chip-sequence is fed to the extracting and de-spreading block where both the main and secret symbols are separated.

The working of this block is explained in the algorithm I. First of all, the extended set of PN-sequence is generated and clusters are formed according to Table II as mentioned earlier. This set of PN sequences is denoted by C. The $RxChips$ are incoming 32 chips PN sequences. The Correlate function calculates the correlation between its two inputs. The result of the correlation between $Rxchips$ and all the sixteen cluster heads goes to $MainCorr$. Function $FindMaxLoc$ calculates the location of maximum value present in the input

of $MainCorr$. If there is more than one maximum value present in that input, then the locations of all the maximum values are returned to Loc as the output. In the case of multiple values in Loc, lets M number of values, the control will go to Line:9 of the algorithm. In this case, the correlation is performed with all sequences of each cluster associated with these locations. Then the sum of the correlation values in all M clusters is calculated and stored in sum_S. One out of these M location for which this sum is maximum is taken in L_M. This location represents the main symbol $Symbol_M$. The secret symbol $Symbol_S$ is the location of the maximum correlation value in $SecCorr[L_M]$ which is the correlation of $RxChips$ with the sequence in the cluster associated with location L_M. If there is only a single value in Loc, then this location itself represents the main symbol. Similarity, the secret symbol is calculated as the sequence from the associated cluster having the maximum correlation with the $RxChips$.

Algorithm 1 Despreading and Extracting Algorithm

1: **procedure** DEA($RxChips, C$)
2: $MainCorr \leftarrow Correlate(RxChips, C_{i,0})$
3: $Loc \leftarrow FindMaxLoc(MainCorr)$
4: **if** Loc = single value **then**
5: $SecCorr \leftarrow Correlate(RxChips, C_{Loc,j})$
6: $Symbol_S \leftarrow FindMaxLoc(SecCorr)$
7: $Symbol_M \leftarrow Loc$
8: **else**
9: **for all** m in Loc **do**
10: $SecCorr[m] \leftarrow Correlate(RxChips, C_{m,j})$
11: $sum_S[m] \leftarrow sum(SecCorr[m])$
12: **end for**
13: $L_M \leftarrow m$ for which sum_S is maximum
14: $Symbol_S \leftarrow FindMaxLoc(SecCorr[L_M])$
15: $Symbol_M \leftarrow L_M$
16: **end if**
17: **return** $Symbol_M, Symbol_S$
18: **end procedure**

After the separation of both types of symbols, the CRC and $SCRC$ are calculated and checked. If CRC is not matched, it indicates the error in the main frame and a $NACK$ is transmitted. If both CRC and $SCRC$ are matched with the corresponding values, then $SACK$ is transmitted. If CRC is correct but not the $SCRC$, it indicates an error in the secret message and a $SNACK$ is transmitted. $SACK$ is an ACK with positive acknowledgment of the secret message while $SNACK$ is a negative acknowledgment for the same.

D. Secret Frame Acknowledgment Scheme

For the purpose of secret acknowledgment, we used 1-bit reserved field which is present in the byte allocated for the length of PHY-layer payload. Only 7 out of the 8 bits are used for denoting the length while the remaining 1-bit can be used for the mentioned purpose. For the $SACK$ frame, the reserve field in the ACK frame is set to one, while it is set to zero for the $SNACK$ frame. The process of the acknowledgment at the receiver is expressed in Table III.

TABLE III: Acknowledgment decision at the receiver

CRC	SCRC	Main Channel	Secret Channel	Reserved Field
Not Correct	X	NACK	X	X
Correct	Not Correct	ACK	SNACK	0
Correct	Correct	ACK	SACK	1

At the transmitter side, it will wait for the $ACK/NACK$ frame transmitted by the receiver. If it gets the $NACK$ frame, it reflects that both the main and the secret symbols have not been received correctly. If it gets ACK frame, then acknowledgment of the secret symbol depends on the reserve field. If it is set to one then it reflects that both types of the symbols have been received correctly. This process is described in Table IV.

TABLE IV: Status of Acknowledgment at the transmitter

ACK/NACK	Reserved Field	Main Data	Secret Data
NACK	X	Corrupted	X Corupted
ACK	0	Correct	Corrupted
ACK	1	Correct	Corrupt

V. Result and Performance Analysis

We have implemented the proposed system in MATLAB and analyzed its performance in terms of Symbol Error Rate (SER) as a performance metric. Results are given in Fig. 5 and notations used in the figures are explained in Table V. In the following subsections, we analyze the performance of the proposed method in terms of stealth, robustness and throughput.

TABLE V: Detail of Notations Used

SER, CER	symbol, chip error rate at standard 802.15.4 without embedding
MSER, MCER	symbol, chip error rate of main data
SSER SCER	symbol, chip error rate of secret data
USER, UCER	symbol, chip error rate at unaware receiver
PMSER, PMCER	symbol, chip error rate of main data with proposed method
PSSER, PSCER	symbol, chip error rate of secret data with poposed method
PUSER, PUCER	symbol, chip error rate at unaware receiver with proposed method

A. Stealth

For the proposed mechanism to be stealth, it should meet to two aspects. First, the presence of the scheme should not be easily detectable. Second, it should not have a noticeable effect on the unaware receiver in recovering process of the messages. To satisfy both these conditions, the modification in the chips sequence should be as low as possible. From the Fig. 5, it can be observed that the symbol error rate at the unaware receiver is better than the existing method. At the same time, we can observe that the main symbol error rate at the known receiver with the proposed method is better which results in less degradation of the main channel with the embedding process.

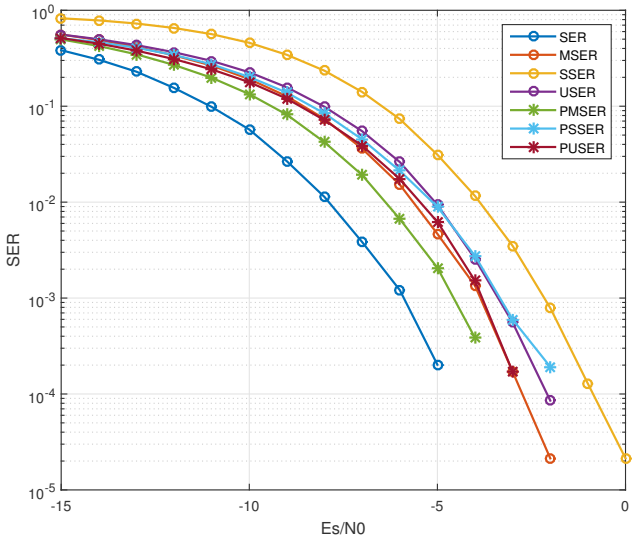

Fig. 5: Comparison of SER

B. Robustness

From Fig. 5, we can observe that the secret symbol error rate is better for proposed method in the noisy environment and hence the proposed method is more robust to adverse channel conditions.

C. Throughput

As proposed method gives the capability of hiding 2 secret bits in per symbol of 4-bits, the proposed method can provide half the data rate of the secret data than that of main data in the favorable channel conditions.

VI. Conclusion

In this paper, we proposed a method to create a covert and reliable channel along with the main channel over 802.15.4. We analyzed the performance of the proposed method and compared it with the existing method for 32 chips DSSS. We proposed a secret acknowledgment method and error detection method to ensure reliable communication in the covert channel. Results show that secret data can be transferred at a significant data rate even in noisy environment. This method is expected to be very useful for transmission of critical sensitive and secret information. The future work can be extended to develop variable size cluster of codes based on available channel quality. More secret bits can be embed per symbol when channel quality is excellent and capacity of the covert channel can be utilized properly. Security of secret data can also be explored in the future work.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015.

[2] J. A. Stankovic, "Research directions for the internet of things", *IEEE Internet of Things J.*, vol. 1, no. 1, pp. 39, 2014.

[3] Y. M. Amin and A. T. Abdel Hamid,"Classification and analysis of IEEE 802.15.4 PHY layer attacks", *2016 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, Cairo, Egypt, 2016, pp. 1-8.

[4] Yulong Zou, Xianbin Wang and Lajos Hanzo, "A survey on wireless security: technical challenges, recent advances and future trends." *arXiv preprint arXiv:1505.07919, May, 2015*.

[5] Cox I. J., Miller M. L., Bloom J. A., Fridrich J., Kalker T.,"Steganography", *Digital Watermarking and Steganography* 2nd ed. Morgan Kaufmann 2008, ch. 12, pp. 425-467.

[6] K. Satish, T. Jayakar, C. Tobin, K. Madhavi and K. Murali, "Chaos based spread spectrum image steganography," in *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 587-590, May 2004.

[7] K. Ntalianis and N. Tsapatsoulis, "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks," in *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 156-174, Jan.-March 2016.

[8] Mukherjee A., et al.,"Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Comm. Surveys & Tutorials*, vol., No. 3, pp. 1550-1573, 2014.

[9] Goeckel, D., Vasudevan, S., Towsley, D., Adams, S., Ding, Z., and Leung, K., "Artificial Noise Generation from Cooperative Relays for Everlasting Secrecy in Two-Hop Wireless Networks, *IEEE J. on Selected Areas in Comm.*, vol. 29, no. 10, pp. 2067-2076, October 2011.

[10] J. Zhang and M. C. Gursoy, "Collaborative Relay Beamforming for Secrecy," *Communications (ICC), 2010 IEEE International Conference on*, Cape Town, 2010, pp. 1-5

[11] A. Mukherjee amd A. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels with Imperfect CSI, *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351-361, January 2011.

[12] D. Martins and H. Guyennet, "Attacks with Steganography in PHY and MAC Layers of 802.15.4 Protocol," in *Fifth International Conference on Systems and Networks Communications*, Nice, 2010, pp. 31-36.

[13] D. Martins and H. Guyennet, "Steganography in MAC Layers of 802.15.4 Protocol for Securing Wireless Sensor Networks," 2010 *International Conference on Multimedia Information Networking and Security*, Nanjing, Jiangsu, 2010, pp. 824-828

[14] B. A. Bash, D. Goeckel, D. Towsley and S. Guha, "Hiding information in noise: fundamental limits of covert wireless communication," in *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26-31, Dec. 2015.

[15] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques, *Selected Areas in Communications, IEEE Journal on*, vol. 28, no. 5, pp. 703715, 2010.

[16] B. Muntwyler, V. Lenders, F. Legendre, and B. Plattner, "Obfuscating ieee 802.15.4 communication using secret spreading codes, in *Wireless On-demand Network Systems and Services (WONS), 2012 9th Annual Conference on. IEEE*, 2012, pp. 18.

[17] T. Kho, "Steganography in the 802.15. 4 physical layer, UC Berkeley, 2007.

[18] X. Li, C. Yu, M. Hizlan, W. T. Kim and S. Park, "Physical Layer Watermarking of Direct Sequence Spread Spectrum Signals," *MILCOM 2013 - 2013 IEEE Military Communications Conference*, San Diego, CA, 2013, pp. 476-481

[19] A. M. Mehta, S. Lanzisera, and K. Pister, "Steganography in 802.15.4 wireless communication, in *Advanced Networks and Telecommunication Systems, 2008. ANTS08. 2nd International Symposium on. IEEE*, 2008, pp. 13.